The following security alert was issued by the Information Security Division of the Mississippi Department of ITS and is intended for State government entities. The information may or may not be applicable to the general public and accordingly, the State does not warrant its use for any specific purposes.

DATE(S) ISSUED:
12/14/2010

SUBJECT:
Vulnerabilities in the OpenType Font (OTF) Driver Could Allow Remote Code Execution (MS10-091)

OVERVIEW:
Multiple vulnerabilities have been discovered in the Microsoft Windows OpenType Font (OTF) driver that could allow for remote code execution. OpenType fonts are fonts that are embedded in documents such as Microsoft Word or used in web pages. The vulnerabilities can be exploited if a user visits a network share with a specially crafted OpenType font. These vulnerabilities are triggered by the Details and Preview panes in Windows Explorer. These vulnerabilities can also be exploited if a user views a specially crafted OpenType font using a third-party web browser. In this scenario, the vulnerability could be triggered if a user views a web page with an embedded, specially crafted OpenType font. Successful exploitation of these vulnerabilities could result in an attacker gaining system-level privileges. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts may result in a denial-of-service condition.

SYSTEMS AFFECTED:
- Windows XP
- Windows Server 2003
- Windows Vista
- Windows Server 2008
- Windows 7
- Windows Server 2008 R2

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **High**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **High**

Home users: High

DESCRIPTION:
Multiple vulnerabilities have been discovered in the Microsoft Windows OpenType Fonts that could allow for remote code execution.

OpenType Font Index Vulnerability
A vulnerability exists due to the OTF driver improperly indexing an array of OpenType fonts.

OpenType Font Double Free Vulnerability
A vulnerability exists due to the OTF driver improperly resetting a pointer when freeing memory.

OpenType CMAP Table Vulnerability
A vulnerability exists due to the OTF driver improperly parsing the CMAP table. The CMAP table defines a mapping between character codes and glyph index values used in the font.

These vulnerabilities can be exploited if a user visits a network share with a specially crafted OpenType font. These vulnerabilities are triggered by the Details and Preview panes in Windows Explorer. These vulnerabilities can also be exploited if a user views a specially crafted OpenType font with a third-party browser. Successful exploitation of this vulnerability could result in an attacker gaining the system-level privileges. An attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Failed exploit attempts may result in a denial-of-service condition.

RECOMMENDATIONS:
The following actions should be taken:

- Apply the appropriate patches provided by Microsoft immediately after appropriate testing.
- Consider disabling the Preview and Details panes in Windows Explorer.

Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.

REFERENCES:

Microsoft:
http://www.microsoft.com/technet/security/bulletin/ms10-091.mspx

CVE:
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3956
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3957
http://www.cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3959